

No. IT- 044	Policy Name: Procedure for Review of User Accounts for Financial Systems
Effective Date: 8-1-2014 Last Revised Date: 8-1-2014	Citywide Policy _ IT Policy _ IT Procedure <u>X</u>
Approved By: IT Director	

**Procedure for Review of User Accounts for Financial Systems**

**PURPOSE:** To ensure appropriate individuals have access to data that is essential to perform their job functions related to financial systems for the City of Hampton.

**Scope:** City of Hampton will perform scheduled periodic reviews of user access for all financially significant applications on at least an annual basis in order to identify unauthorized/inappropriate access based on job function, as well as to identify any terminated users who have remained active in the application. System generated lists of users should be sent to the appropriate Supervisor for review. The systems with user reviews that fall within this policy include the following:

- o Financial System including A/P, A/R, General Ledger, etc.
- o Procurement
- o Payroll

Tax & Revenue System

**POLICY:** IT-021 IT Security Policy

**PROCEDURE:** Reviews will take a combination approach to ensure users are appropriate and their permissions are appropriate for their job duties. Reviews of users of financial systems accounts will take place on an ongoing basis as well as an annual basis.

**Ongoing Process:**

**Financial, Tax and Revenue System:**

1. The IT Department will access a listing of all users at least every month.
2. The IT Department will identify users that have not logged on in over 6 months. Any user that has not logged on in over 6 months will be flagged for inquiry.
3. IT will open a ticket to track all the flagged for inquiry users for a given month.
4. IT will contact the department and produce a listing of all current users flagged for inquiry to verify the user is still valid or if they should be removed from access. Documentation on the contact with the department will be through e-mail.
5. Termination and transfers will follow IT procedure IT-035 IT Process for Employee Transfers, Terminations and Employee Related Security Threats
6. IT will update the ticket with the user changes and any documentation. Once all changes have been made for the month the ticket will be closed.

**Payroll System:**

System rules are set to terminate users that have no activity within 90 day

**Annual Process:**

1. Once per year between January and March, information will be gathered from departments through a form. The purpose will be to verify that permissions for users are still appropriate and valid. The form will gather the following information:
  - a. Verify Employee Name
  - b. Verify Employee Department
  - c. Verify Employee Access and Permissions
  - d. Identify and Document Changes Needed to Employee Access and Permissions
2. The list will be distributed to department heads for review and comment.
3. Department heads will send the list back to IT with their changes.
4. Any employees identified by the department that has been terminated or transferred to another department will be changed appropriately. The IT department will have access changed following Procedure IT-035 IT Process for Employee Transfers, Terminations and Employee Related Security Threats.
5. Any employees found to need access and permission changes, the IT department will make those changes and use the forms received by departments as documentation of authorization to make the change.
6. IT Department staff assigned to make permission changes will open a ticket and document the changes and time the changes were made.
7. IT Department staff will notify department heads when changes have been completed